

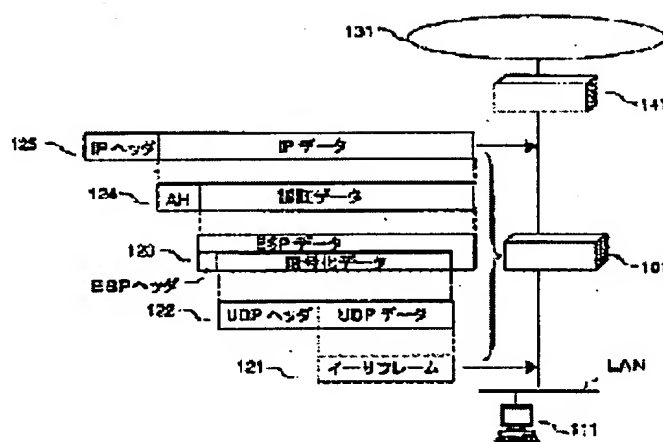
TUNNELING DEVICE

Patent number: JP2002271417
Publication date: 2002-09-20
Inventor: TERADA KIYONOBU; KAJIWARA MASAFUMI
Applicant: HITACHI CABLE; OSAKA MEDIA PORT CORP
Classification:
 - International: H04L12/66; G06F13/00; G06F15/00; H04L12/46; H04L12/56
 - european:
Application number: JP20010061941 20010306
Priority number(s): JP20010061941 20010306

[Report a data error here](#)

Abstract of JP2002271417

PROBLEM TO BE SOLVED: To provide a tunneling device which is capable of operating LANs through an IP network as a common VPN. **SOLUTION:** An LAN-side port has a function of receiving the entire frame 121 of a data link layer flowing through a network, forming (encapsulated) an IP packet 125 that contains the received frame as data, and transmitting the IP packet 125 from the IP network-side port to a tunneling terminal station. An IP network-side port has a function of receiving the IP packet 125 addressed to it, taking out the frame 121 of the data link layer from the IP packet 125 when the IP packet 125 is the encapsulated frame of the data link layer, and transmitting the frame 121 from the LAN-side port.



Data supplied from the *esp@cenet* database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-271417

(P2002-271417A)

(43) 公開日 平成14年9月20日 (2002.9.20)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 5
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 B 5 B 0 8 9
	15/00	15/00	3 1 0 5 K 0 3 0
H 0 4 L 12/46	2 0 0	H 0 4 L 12/46	2 0 0 X 5 K 0 3 3
12/56		12/56	H
審査請求 未請求 請求項の数 2 O L (全 10 頁)			

(21) 出願番号 特願2001-61941(P2001-61941)

(22) 出願日 平成13年3月6日 (2001.3.6)

(71) 出願人 000005120

日立電線株式会社

東京都千代田区大手町一丁目6番1号

(71) 出願人 597056121

大阪メディアポート株式会社

大阪府大阪市北区中之島6丁目2番27号

(72) 発明者 寺田 清伸

茨城県日立市日高町5丁目1番1号 日立

電線株式会社オプトロシステム研究所内

(74) 代理人 100068021

弁理士 絹谷 信雄

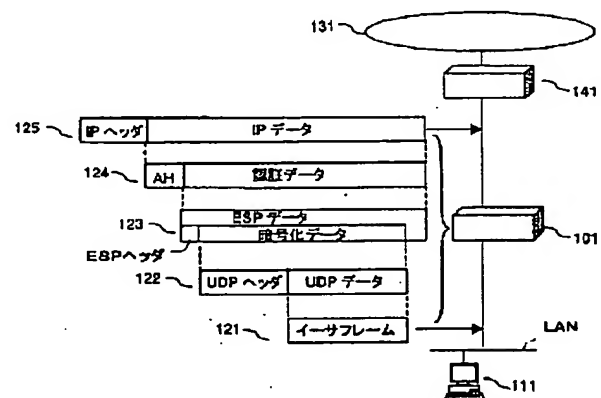
最終頁に続く

(54) 【発明の名称】 トンネリング装置

(57) 【要約】

【課題】 IP網を介したLAN同士を共通のVPNとして運用可能とするトンネリング装置を提供する。

【解決手段】 LAN側ポートでは、ネットワークを流れるデータリンク層のフレーム121全てを受信し、その受信したフレームをデータとするIPパケット125を作成(カプセル化)し、そのパケットをIP網側ポートからトンネリングの終端局宛てに送信する機能を備え、IP網側ポートでは、自局宛てに送られてきたIPパケット125を受信し、そのIPパケット125がデータリンク層のフレームをカプセル化したものである場合には、そのIPパケット125からデータリンク層のフレーム121を取り出し、そのフレーム121をLAN側ポートから送信する。



【特許請求の範囲】

【請求項1】 OSI参照モデルのデータリンク層のフレームを送受信することができるLAN側ポートとOSI参照モデルのネットワーク層のフレーム（パケット）を送受信することができるIP網側ポートとを備え、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のIPアドレスを登録するバッファ部を備え、前記LAN側ポートでは、ネットワークを流れるデータリンク層のフレーム全てを受信し、その受信したフレームをデータとするIPパケットを作成（カプセル化）し、そのパケットをIP網側ポートからトンネリングの終端局宛てに送信する機能を備え、前記IP網側ポートでは、自局宛てに送られてきたIPパケットを受信し、そのIPパケットがデータリンク層のフレームをカプセル化したものである場合には、そのIPパケットからデータリンク層のフレームを取り出し、そのフレームをLAN側ポートから送信する機能を備えたことを特徴とするトンネリング装置。

【請求項2】 前記LAN側ポートにおいて受信したデータリンク層フレームをカプセル化する際に、データの内容を暗号化し、その暗号化したデータに暗号化方式などを設定した暗号化ヘッダを付加し、さらに送信者の正当性を証明する認証ヘッダを付加する機能を備え、前記IP網側ポートにおいて受信したIPパケットからデータリンク層のフレームを取り出す際に、そのIPパケットに認証ヘッダが含まれている場合にはその認証ヘッダによりIPパケット送信者の正当性やデータ改竄の有無を検証し、さらに前記IPパケットに暗号化ヘッダが含まれている場合には暗号化されているデータを復号化する機能を備えたことを特徴とする請求項1記載のトンネリング装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、広域の各地に点在する事業所や大学等のローカルエリアネットワークを専用線に比べて低コストなIP網を使って接続し、仮想的なプライベートネットワークを構成するVPN技術に係り、特に、企業や大学、ISP等に設置して使用するVPN装置のためのトンネリング装置に関するものである。

【0002】

【従来の技術】端末が互いに遠隔地に存在するネットワークを安全に接続するためのVPN方式としてRFC2401等で規定されるIPsecを使用したもの、RFC2661で規定されるL2TPを使用したもの、RFC2547で規定されるMPLSを使用したものの3つの方式が一般的に知られている。

【0003】まず、図4を用いてIPsecを使用した方式について述べる。LAN421、422をIP網431を介して仮想的なプライベートネットワークとして

安全に接続するため、IPsec機能を搭載したルータ441、442を使って接続する。端末411～412と端末413～414との間で送受信されるパケットは、ルータ441、442によってIPsecの暗号化及び認証が行われ、インターネット上では図14のAHヘッダが付加された状態、または図15のESPペイロードフォーマットによりカプセル化された状態、またはその両方の状態でパケットが転送される。これにより、LAN421、422間の通信内容がネットワーク上の第三者による盗聴やパケットの改竄から保護され、各端末が安全に通信を行うことができる。

【0004】次に、図5を用いてL2TPを使用した方式について述べる。この方式では、VPN接続を行う端末は、まず電話回線523を使用してLAC571にPPPで接続する。LAC571は、このPPPフレームに図16に示すL2TPヘッダを付加してL2TPフレームとした後、このL2TPフレームをIP網531を経由してルータ542へパケットとして転送する。ルータ542はLNSと呼ばれ、このL2TPフレームをLAN522のフレームフォーマットに変換し、LAN522上の端末に転送する。また、電話回線523を使用しない場合、上記LAC機能を備えた専用ソフトを搭載した端末512（LACクライアント）は、上記LAC571と同様にPPPフレームにL2TPヘッダを付加し、そのL2TPフレームをLAN522に転送し、LAN522上の端末と通信を行う。これにより、IP網上でLACまたはLACクライアントからLNSまでに仮想的なポイントトゥポイントコネクションが張られ、IP網を介して端末511、512をプライベートネットワークであるLAN522に安全に接続することができる。

【0005】次に、図6を用いてMPLSを使用した方式について述べる。LANとIP網とを接続するルータ641、642はLE (Label edge) ルータと呼ばれ、図17に示すシムヘッダを付けてフレームを転送する機能を持つ。また、IP網内はシムヘッダ内のラベルに従ってパケットを交換する機能を持つLSR (Label Switch router) 643～645で接続する。端末611から端末613に送信されたフレームは、LEルータ641によってシムヘッダが付加され、パケットとしてIP網に送信された後、シムヘッダ内のラベルに従ってLSR643～645によって転送される。そのパケットがLEルータ642まで到達すると、LEルータ642はこのシムヘッダを取り外し、フレームを端末613に転送する。LSR間で行われるパケット転送は、ネットワークアドレスではなくLE641で付けられたラベルのみを参照して行われるため、他のネットワークから送信されたパケットが転送されることがなく、LAN621とLAN622との間の通信が保護される。

【0006】ここで、本明細書に使用される略語の日本

語表記又は簡単な説明を列記しておく。

【0007】OSI(Open Systems Interconnection)参照モデル：国際標準化機構が定める開放型システム間相互接続参照モデル。2層はデータリンク層、3層はネットワーク層、4層はトランスポート層と呼ばれる。

【0008】IP(Internet Protocol)：インターネットプロトコル(ネットワーク層)

TCP/IP(Transport-Control Protocol/Internet Protocol)：インターネットの標準プロトコル群

UDP(User Datagram Protocol)：コネクションレス型のトランスポート層プロトコル

TCP(Transmission Control Protocol)：コネクション型のトランスポート層プロトコル

VPN(Virtual Private Network)：仮想私設網

ISP(Internet Service Provider)：インターネットサービスプロバイダ

RFC(Request for Comments)：インターネットアーキテクチャ委員会による標準勧告文書、2401、2661、2547などはその文書の番号

IPsec(IP security)：インターネットプロトコルセキュリティ

ESP：IPsecにより作成した暗号化データ、ヘッダを示す名称

L2TP(Layer Two Tunneling Protocol)：レイヤ2トンネリングプロトコルMPLS(Multi Protocol Label Switching)：マルチプロトコルラベルスイッチング

LAC(L2TP Access Concentrator)：L2TPアクセスコントローラ

PPP(Point to Point Protocol)：公衆回線でIP接続するためのプロトコル

LNS(L2TP Network Server)：L2TPネットワークサーバ

IEEE(Institute of Electrical and Electronics Engineers)：アメリカ電気・電子技術者協会

IPv6(IP version 6)：アドレス長を長くしたIP

NetBIOS(Network Basic Input/Output System)：ネットワーク基本入力システム

IPX(Internetwork Packet Exchange)：ノベル社のネットワーク層プロトコル

AppleTalk：アップル社のネットワークOS
以上に列記しないものも含め本明細書に使用される略語、用語は、いずれも公知の文献に記載されているものであり、本明細書では詳細な説明は省略する。

【0009】

【発明が解決しようとする課題】従来技術において、IPsecを使用した方式では、ネットワーク層においてIPパケットの暗号化とカプセル化とを行うため、通信可能なプロトコルがIPに限定されてしまう。

【0010】また、L2TPを使用した方式では、クライアントがPPP接続しているか、または専用ソフトを

使用しなければならず、特定のクライアントしかVPNを利用することができない。

【0011】また、MPLSを使用した方式では、MPLSに対応したルータで構成されたネットワーク内でしか通信できないという問題がある。

【0012】そこで、本発明の目的は、上記課題を解決し、IP網を介したLAN同士を共通のVPNとして運用可能とするトンネリング装置を提供することにある。

【0013】

【課題を解決するための手段】上記目的を達成するために本発明は、OSI参照モデルのデータリンク層のフレームを送受信することができるLAN側ポートとOSI参照モデルのネットワーク層のフレーム(パケット)を送受信することができるIP網側ポートとを備え、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のIPアドレスを登録するバッファ部を備え、前記LAN側ポートでは、ネットワークを流れるデータリンク層のフレーム全てを受信し、その受信したフレームをデータとするIPパケットを作成(カプセル化)し、そのパケットをIP網側ポートからトンネリングの終端局宛てに送信する機能を備え、前記IP網側ポートでは、自局宛てに送られてきたIPパケットを受信し、そのIPパケットがデータリンク層のフレームをカプセル化したものである場合には、そのIPパケットからデータリンク層のフレームを取り出し、そのフレームをLAN側ポートから送信する機能を備えたものである。

【0014】前記LAN側ポートにおいて受信したデータリンク層フレームをカプセル化する際に、データの内容を暗号化し、その暗号化したデータに暗号化方式などを設定した暗号化ヘッダを付加し、さらに送信者の正当性を証明する認証ヘッダを付加する機能を備え、前記IP網側ポートにおいて受信したIPパケットからデータリンク層のフレームを取り出す際に、そのIPパケットに認証ヘッダが含まれている場合にはその認証ヘッダによりIPパケット送信者の正当性やデータ改竄の有無を検証し、さらに前記IPパケットに暗号化ヘッダが含まれている場合には暗号化されているデータを復号化する機能を備えてもよい。

【0015】

【発明の実施の形態】以下、本発明の一実施形態を添付図面に基づいて詳述する。

【0016】図1に示されるように、本発明に係るトンネリング装置101は、LAN側の伝送路に接続されるLAN側ポートとIP網131側の伝送路に接続されるIP網側ポートとを備え、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のIPアドレスを登録するバッファ部を内部に備えている。

【0017】このトンネリング装置101は、LANから受信したデータリンク層のフレーム(ここではイーサ

ネット（登録商標）フレーム：イーサフレームともいう）121をUDPデータとし、このUDPデータにUDPヘッダを付加してフレーム122を作成するUDPフレーム作成手段と、このUDPヘッダを含むフレーム122全体を所定の暗号化方式（ここではIPsecに基づく暗号化方式）で暗号化し、この暗号化データにESPヘッダ及びトレーラを付加してフレーム（ESPデータ）123を作成する暗号化手段と、このフレーム123にこのフレーム123を認証データとする認証ヘッダ（ここではAHヘッダ）を付加してフレーム124を作成する認証情報付加手段と、このフレーム124をIPデータとし、このIPデータにバッファ部に登録されているIPアドレスを用いたIPヘッダを付加してネットワーク層のフレーム（IPパケット）125を作成（カプセル化）するカプセル化手段とを備える。

【0018】また、このトンネリング装置101は、IP網131から受信したネットワーク層のフレーム（IPパケット）が上記カプセル化によるIPパケット125であることを認識するカプセル化認識手段と、そのIPデータであるフレーム124に含まれている認証ヘッダを認識して認証データの認証を行う認証手段と、その認証データ（フレーム123）に含まれている暗号化ヘッダを認識して暗号化データを復号化してUDPフレーム122を復元する復号化手段と、そのUDPフレーム122からデータリンク層のフレーム121を取り出すフレーム取出手段とを備える。

【0019】111はLANに接続された端末、141はIP網131との中継を行うルータである。図1には、トンネリング装置101が1つしか示されていないが、IP網131に複数のトンネリング装置101が繋がることにより、トンネリング装置相互間の送受信が実現できる。その例を図2により説明する。

【0020】図2において、LAN221は事業所Aのイーサネット、LAN222は事業所Bのイーサネット、IP網231はインターネット、201、202は、本発明に係るトンネリング装置、241、242はルータである。トンネリング装置201、202のIP網側ポート251、254はルータ241、242にそれぞれ接続され、IP網側ポート251、254のデータリンク層の通信媒体はイーサネットである。LAN側ポート252、253は、LAN221、222にそれぞれ接続されている。LAN221、222の端末211～214にはTCP/IPプロトコルが実装されている。

【0021】各端末211～214、各トンネリング装置201、202及び各ルータ241、242のインタフェースのIPアドレス及びMACアドレスは図7のようになっているものとする。ただし、図7において、「インタフェース」と書かれている欄は、図2における各部材の符号を示している。従って、例えば、端末21

1のMACアドレスは、“00：00：00：00：00：01”、IPアドレスは、“192.0.0.1/24”である。

【0022】トンネリング装置201、202のUDPポート番号は、“1701”に設定されているものとする。

【0023】トンネリング装置201、202のソフトウェア構成は、図8のようになっているものとする。即ち、トンネリング装置201、202は、ソフトウェアとして少なくとも、LAN側ポート及びIP網側ポートにおけるイーサネットに係る処理を行うイーサネットドライバと、TCP/IP及びIPsecソフトウェアと、本発明に係るトンネリングソフトウェアとを備える。図1で説明した各手段は、これらのソフトウェアで実現されている。

【0024】トンネリング装置201、202のハードウェア構成は、図18のようになっているものとする。即ち、トンネリング装置201、202は、OS参照モデルのデータリンク層のフレームを送受信することができるLAN側ポート1801と、OS参照モデルのネットワーク層のフレームを送受信することができるIP網側ポート1802と、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のIPアドレスを登録するバッファ部を含む主記憶装置1803と、図8のソフトウェアを実行するCPU1804と、補助記憶装置1805とを有する。

【0025】図2のように場所などが異なる2つのLAN221、222をVPN接続し、端末211と端末213との間で安全に通信する本発明の手順を以下に述べる。なお、本実施形態では、VPNのセキュリティ機能を提供する手段として、通信路上のデータの暗号化及び認証を行うIPsecを利用した。

【0026】まず、端末211から端末213へ宛ててLAN221へフレームが送信されたものとする。

【0027】トンネリング装置201は、LAN221を流れるフレームを宛先に関わらず全てプロミスキャス（無差別）に受信し、受信したフレーム（図1のフレーム121）に宛先ポート番号を“1701”に設定したUDPヘッダを付加する（フレーム122）。UDPヘッダは、図12に示すフォーマットで作成される。図12において、1201が宛先ポート番号“1701”を格納するフィールドである。

【0028】次に、トンネリング装置201は、UDPフレーム122全体を暗号化し、ESPヘッダ及びトレーラを付加してESPデータ（フレーム123）を作成する。ESPペイロードは、図15に示すフォーマットで作成される。

【0029】次に、トンネリング装置201は、パケットの正当性を証明するAHヘッダを付加する（フレーム124）。AHヘッダは、図14に示すフォーマットで

作成される。

【0030】次に、トンネリング装置201は、自局（トンネリング装置201）をトンネリングの始点としたときのトンネリングの終点となる終端局（ここではトンネリング装置202）のIPアドレスをバッファ部の内容（図7）から判定し、IP網側ポート254のIPアドレス“20.0.0.2/24”を用いてトンネリング装置202を宛先とするIPヘッダを作成し、このIPヘッダをフレーム124に付加することにより、IPパケット（フレーム125）を作成する。IPヘッダは、図11に示すフォーマットで作成される。図11において1101が宛先IPアドレスを格納するフィールドである。トンネリング装置201は、このフレーム125をIP網側ポート251からルータ241のポート261へ送信する。

【0031】なお、IP網側ポート251に接続するデータリンク層の通信方式（通信媒体）はイーサネットであるため、IP網側ポート251から実際に送信されるフレームの形式は、作成されたIPパケット（フレーム125）をデータとして、図9のIEEE802.2/802.3カプセル化又は図10のイーサネットカプセル化が行われた形式となる。図9、10において、901、1001がIPパケットをデータとして格納するフィールドである。

【0032】ルータ241のポート262よりIP網23-1に送信されたIPパケットは、ルータ242のポート263へ到着し、ポート264よりトンネリング装置202のIP網側ポート254に送信される。

【0033】トンネリング装置202は、IP網から自局のUDPポート“1701”宛てのIPパケット（フレーム125）（IPヘッダに格納されている宛先IPアドレスが“20.0.0.2/24”）を受信した場合、フレーム124のAHヘッダによりパケットの正当性を確認し、フレーム123のESPデータの復号化を行い、フレーム122のUDPヘッダを取り除いて元のイーサネットフレーム（フレーム121）を取り出し、そのフレームをLAN側ポート253からLAN222に送信する。

【0034】このフレームは、端末213に到着する。このようにして、端末211から送信されたフレームが端末213に受信される。

【0035】端末213から端末211へ宛ててLAN222へフレームが送信された場合についても、トンネリング装置202がトンネリング装置201と同様に、LAN側ポート253で受信したフレームを前述と同様の処理（IPsec処理、ヘッダ付加処理）によりカプセル化した後、トンネリング装置201のUDPポート（番号1701）に宛ててIP網側へ送信する。トンネリング装置201は、IP網側から自局のUDPポート（番号1701）で受信したIPパケットから前述と同

様の処理（IPsec処理、ヘッダ除去処理）によりイーサネットフレームを取り出した後、そのフレームをLAN側ポート252からLAN221に送信する。こうして、端末213から送信されたフレームが端末211に受信される。

【0036】なお、本実施形態では、UDPポート番号として1701番を使用しているが、他の番号でも構わない。

【0037】また、本実施形態では、データリンク層のフレームにUDPヘッダとIPヘッダとを付加したが、TCPヘッダとIPヘッダとを付加してもよく、或いは独自のトランスポート層ヘッダとIPヘッダとを付加してもよく、或いはIPヘッダのみを付加してもよい。TCPヘッダのフォーマットは、図13に示すとおりである。

【0038】ここで、端末211が端末213宛てのイーサネットフレームを送信した場合の具体的な例として、端末211が端末213のMACアドレスを解決するためにARP要求フレームをLAN221内の全端末にブロードキャスト送信した場合について説明する。端末211が送信したARP要求フレームは、トンネリング装置201によってカプセル化されトンネリング装置202へ転送される。トンネリング装置202は、取り出したARP要求フレームをLAN222内の全端末にブロードキャスト送信する。端末213は、このARP要求フレームを受信すると、ARP応答フレームを端末211宛てにユニキャスト送信する。このARP応答フレームは、トンネリング装置202によってカプセル化されトンネリング装置201へ転送される。トンネリング装置201は、取り出したARP応答フレームをLAN221にユニキャスト送信する。端末211は、このARP応答フレームを受信することになる。

【0039】本発明によれば、IPsecの暗号化によりインタフェース上のデータは保護され、認証によりLAN221、222以外のネットワークからの接続を拒否できるので、LAN221とLAN222との間でVPNを構築することが可能となる。また、このときLAN221、222は、ハブやスイッチで接続されている同じLANセグメントと等価である。

【0040】本実施形態では、場所などが異なる2つのイーサネットを同じIPサブネットとしてVPNを構築したが、イーサネットではない他のデータリンク層の通信方式であっても、また、IP以外のネットワーク層プロトコルを使用した場合であっても、本発明によりVPNを構築することができる。

【0041】また、図3に示すように、端末311～312のデフォルトゲートウェイをルータ341に設定し、ハブやスイッチを使用してトンネリング装置301を介さずにイーサネットフレームを直接ルータ341に送信することにより、LAN321上の端末311～3

12がトンネリング装置を介していないインターネット上の端末(例えば、313~314)と通信を行うことが可能である。このように、本発明のトンネリング装置を用いたネットワークは、相手側のネットワークに本発明のトンネリング装置が存在しない場合でも、相手側のネットワークとの通信が可能である。

【0042】

【発明の効果】本発明は次の如き優れた効果を発揮する。

【0043】(1)請求項1の発明により、トンネリング装置で接続される2つのLANは、間にIP網を介しているにも関わらず、ハブやスイッチで接続されたのと同様に、同一のネットワークとして振る舞うことができる。

【0044】(2)請求項1の発明は、IPsecを使用した方式とは異なり、2つのLANをネットワーク層ではなくデータリンク層で接続するため、2つのLAN間に使用するネットワーク層のプロトコルは、IPプロトコルに限定されず、IPv6やNetBIOS、IPX、AppleTalk等のあらゆるプロトコルの通信が可能となる。

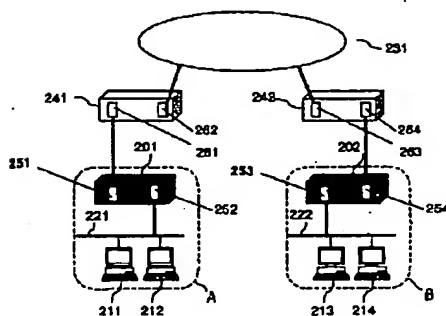
【0045】(3)請求項2の発明のように、IPsec等のセキュリティ機能を組み込むことによって2つのLAN間の通信内容をネットワーク上の第三者による盗聴やパケットの改竄から防ぎ、パブリックなIP網を介していながら安全に接続することが可能である。

【0046】(4)請求項2の発明は、L2TPを使用した方式とは異なり、PPP接続や専用ソフトも必要ない。また、MPLSを使用した方式のようにIP網上のルータをMPLS専用のルータに置き換えたり設定変更する必要もない。なお、セキュリティの強度に関してはIPsecを使用した方式と同等になる。

【図面の簡単な説明】

【図1】本発明の一実施形態を示すトンネリング装置の構成図である。

【図2】



【図2】本発明のトンネリング装置を用いたネットワークの構成図である。

【図3】本発明のトンネリング装置を用いたネットワークの構成図である。

【図4】IPsec方式によるVPNの構成図である。

【図5】L2TP方式によるVPNの構成図である。

【図6】MPLS方式によるVPNの構成図である。

【図7】図2のネットワークにおける各機器のアドレス割り当て図である。

【図8】図1のトンネリング装置のソフトウェア構成図である。

【図9】本発明によるIPパケットをIEEE802.2/802.3カプセル化したフレームの構成図である。

【図10】本発明によるIPパケットをイーサネットカプセル化したフレームの構成図である。

【図11】IPヘッダの構成図である。

【図12】UDPヘッダの構成図である。

【図13】TCPヘッダの構成図である。

【図14】IPsecで用いるAHヘッダの構成図である。

【図15】IPsecで用いるESPペイロードの構成図である。

【図16】L2TPヘッダの構成図である。

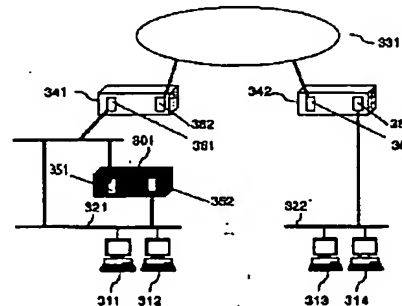
【図17】MPLSで用いるシムヘッダの構成図である。

【図18】図1のトンネリング装置のハードウェア構成図である。

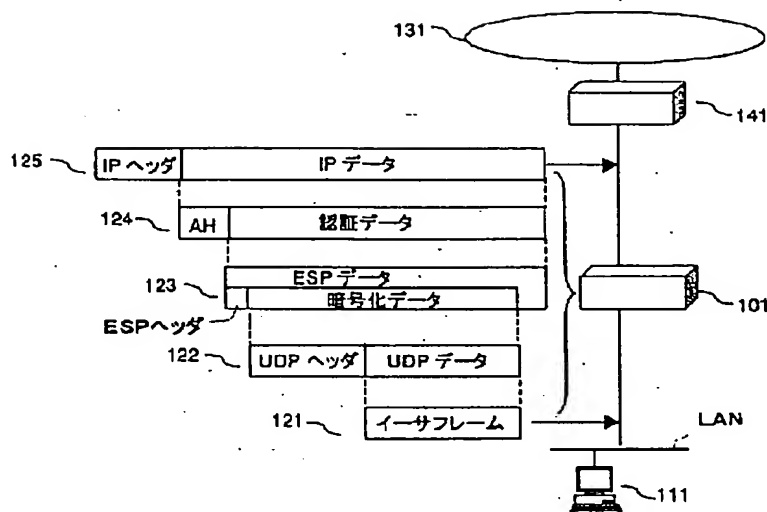
【符号の説明】

101、210、202、301 トンネリング装置
131、231、331 IP網
221、222、321、322 LAN
251、254、351、1802 IP網側ポート
252、253、352、1801 LAN側ポート
1803 バッファ部

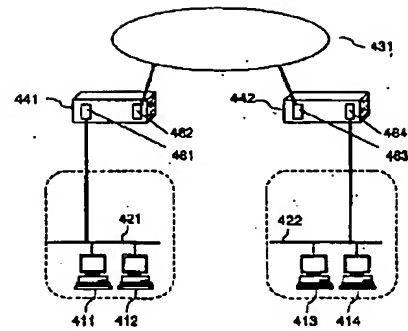
【図3】



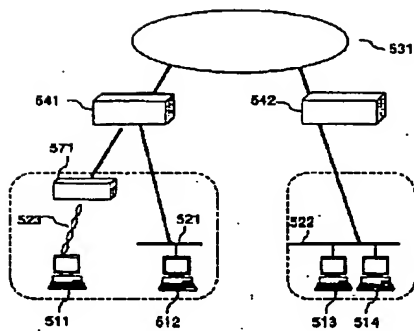
【図1】



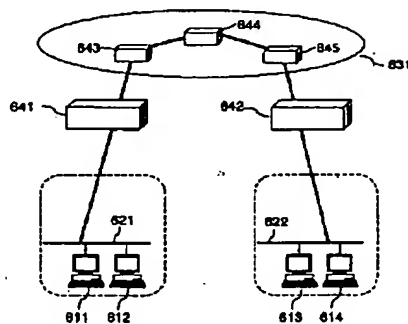
【図4】



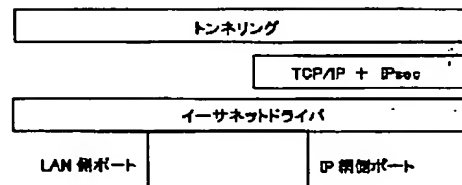
【図5】



【図6】



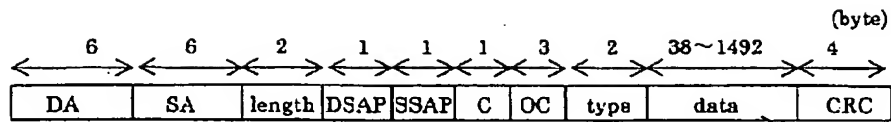
【図8】



【図7】

インタフェース	MACアドレス	IPアドレス
211	00:00:00:00:00:01	192.0.0.1/24
212	00:00:00:00:00:02	192.0.0.2/24
213	00:00:00:00:00:03	192.0.0.3/24
214	00:00:00:00:00:04	192.0.0.4/24
221	00:00:00:00:00:05	10.0.0.1/24
222	00:00:00:00:00:06	なし
223	00:00:00:00:00:07	なし
224	00:00:00:00:00:08	20.0.0.1/24
221	00:00:00:00:00:09	10.0.0.3/24
222	00:00:00:00:00:0a	1.0.0.1/24
223	00:00:00:00:00:0b	2.0.0.1/24
224	00:00:00:00:00:0c	20.0.0.2/24

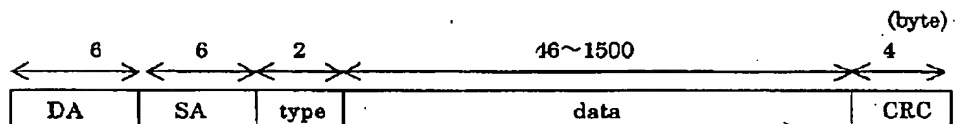
【図9】



DA : Destination Address
 SA : Source Address
 DSAP : Destination Service Access Point
 SSAP : Source Service Access Point
 C : Control
 OC : Original Code
 CRC : Cyclic Redundancy Check

901

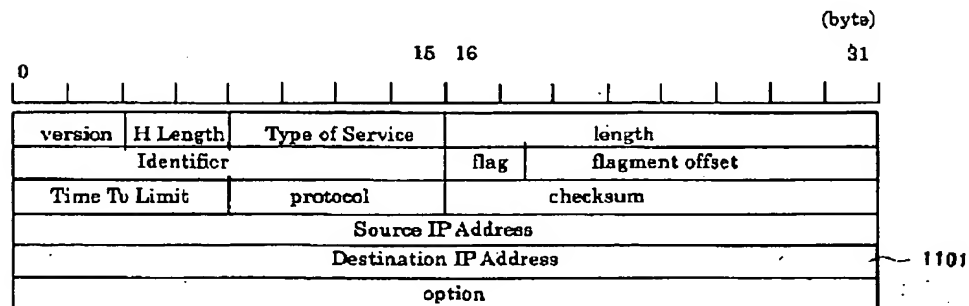
【図10】



DA : Destination Address
 SA : Source Address
 CRC : Cyclic Redundancy Check

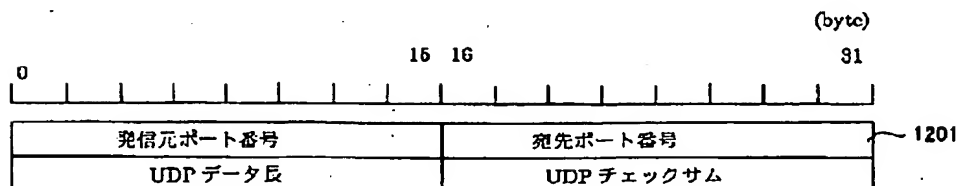
1001

【図11】



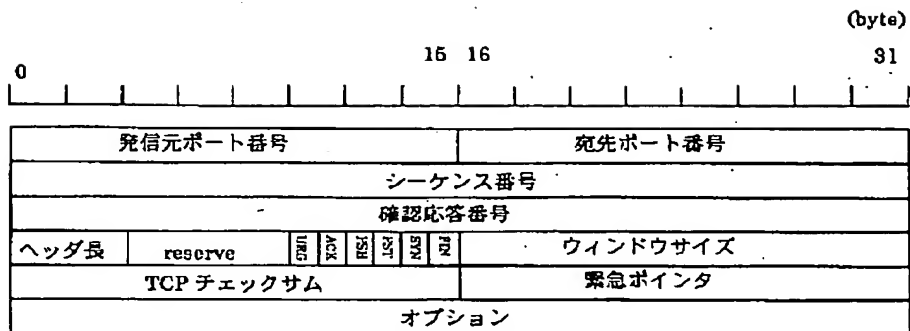
1101

【図12】

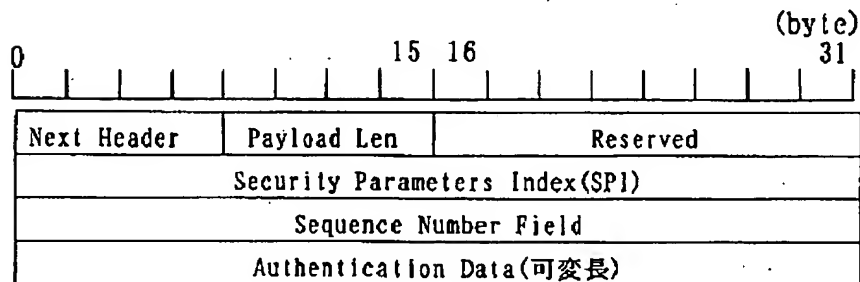


1201

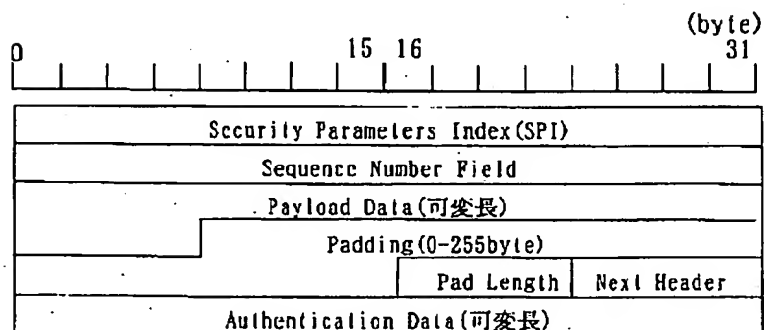
【图 13】



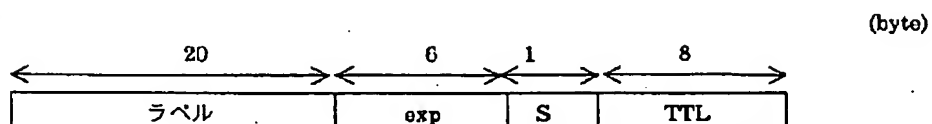
【图 1 4】.



【图 1-5】

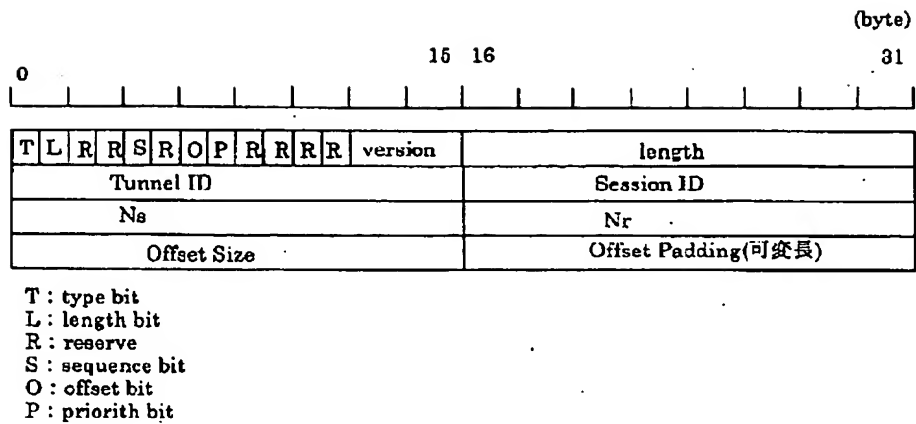


【图 17】

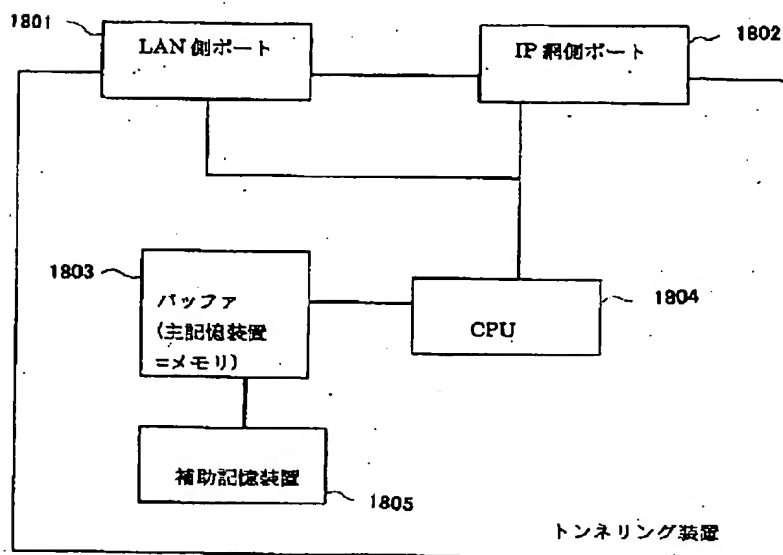


exp: 実験用
S: ラベルスタックの最後を指定
TTL: Time To Live

【例 16】



【图 18】



フロントページの続き

(72)発明者 梶原 将文
大阪府大阪市北区中之島6丁目2番40号
大阪メディアポート株式会社内

Fターム(参考)	5B085	AE00	AE29	BA07	BC07				
	5B089	GA04	GA31	HA06	HA10	HB19			
		JB24	KA04	KA09	KB04	KB06			
		KC28	KC47	KD01	KE02	KE03			
		KF05	KH04	KH30					
	5K030	GA15	HA08	HB18	HC01	HD03			
		HD06	HD09	JA05	KA13	LA07			
		LD19	LE11						
	5K033	AA09	BA02	CA08	CB08	CB11			
		CC01	CC04	DA06	DB10	DB19			